What is claimed is

1. A method for managing a network, comprising the steps of:

detecting occurrence of a network event, said network event having associated with it a network condition comprising at least one of an unplanned macro-event and a planned macro-event related to at least one of a network element and a communication link of said network;

classifying said network event as being at least one of a network element failure, a communications link failure, and a security breach; and

identifying said network event as a network degradation event in response to at least one network event exceeding a network degradation threshold.

2. The method of claim 1, further comprising the step of:

sending an alert to normalize said network degradation event.

3. The method of claim 1, wherein said network event is associated with at least one of a network management system, a security management system, and a system timer.

4. The method of claim 1, wherein said step of identifying comprises the step of:

defining said network degradation event as a brink of failure (BOF) event in an instance where said event is at least one of a type determined to cause a failure of at least one network element within a predetermined time interval, to affect at least one of a critically defined network functionality, and to affect a number of end users exceeding a predetermined threshold level.

5. The method of claim 4, wherein said step of identifying said network degradation event comprises the step of:

assessing at least one of failure rates, mean-time-between-failures (MTBF), mean-time-to-repair (MTTR), and spare parts availability for at least one of network elements and communication links associated with said network event.

6. The method of claim 1, wherein in response to the step of classifying said network event, said method further comprises the steps of:

updating an existing conditions database with indicia of said network event;

determining a latest network topology associated with said network event; and

updating a network topology database with said latest network topology.

7. The method of claim 4, wherein said step of identifying further comprises the step of:

defining said network degradation event as a breach-of-security (BOS) event in an instance where said network event exploits a security vulnerability resulting in at least one of an unauthorized access, an unauthorized modification or compromise, a denial of access to information, a denial of access to network monitoring capability, and a denial of access to network control capability.

8. The method of claim 7, wherein said step of defining said network degradation event as a brink-of-failure (BOF) event further comprises the step of:

correlating network events stored in said existing conditions database with information stored in said network topology database and events stored in a scheduled events database.

9. The method of claim 8 further comprising the steps of:

determining whether said BOF event also causes a BOS event;

determining whether said BOS event also causes a BOF; and

reporting at least one of said BOF event and BOS event.

10. The method of claim 9 further comprising the steps of:

categorizing said BOF event;

determining at least one corrective action procedure associated with said BOF event; and

reporting at least one of a network element and a communications link associated with said BOF event, and said at least one corrective action procedure.

11. The method of claim 10, wherein said step of determining at least one corrective action procedure comprises the step of assessing a BOF database comprising historical information associated with global network reliability practices.

12. The method of claim 9, wherein in an instance where said network degradation event is associated with a breach-of security event, said method further comprises the steps of:

categorizing said breach of security event;

determining at least one corrective action procedure associated with said breach of security event; and

displaying at least one of a network element and a communications link associated with said breach-of security event, and said at least one corrective action procedure.

13. The method of claim 12, wherein said step of determining at least one corrective action procedure comprises the step of assessing a Security Vulnerabilities and Procedures database comprising at least one of historical information of said network and associated global security vulnerabilities and procedures.

14. The method of claim 1, wherein said step of identifying a network event comprises the step of identifying events associated with at least one of end-user data traffic, in-band control traffic, out-of-band control traffic, in-band network management traffic, and out-of-band network management traffic.

15. The method of claim 9 further comprising the steps of:

initiating a new network event upon resolving said network degradation event;

removing said network degradation event from said existing conditions database; and

reporting said network degradation event as a resolved event.

16. The method of claim 15, wherein resolving said network degradation event further comprises the step of at least one of:

resolving said BOF event, such that the BOF event and a BOS condition are cleared; and

resolving said BOS event, such that the BOS event and a BOF condition are cleared.

17. A method for managing a network, comprising the steps of:

detecting occurrence of a network event, said network event having associated with it a network condition comprising at least one of an unplanned macro-event and a planned macro-event related to at least one of a network element and a communication link of said network;

classifying said network event as being at least one of a network element failure, a communications link failure, and a security breach;

identifying said network event as a network degradation event in response to at least one network event exceeding a network degradation threshold by defining said network degradation event as a brink of failure (BOF) event in an instance where said event is at least one of a type determined to cause a failure of at least one network element within a predetermined time interval, to affect at least one of a critically defined network functionality, and to affect a number of end users exceeding a predetermined threshold level; and

sending an alert to normalize said network degradation event.

18. The method of claim 17, wherein said step of identifying further comprises the step of:

defining said network degradation event as a breach-of-security (BOS) event in an instance where said network event exploits a security vulnerability resulting in at least one of an unauthorized access, an unauthorized modification or compromise, a denial of access to information, a denial of access to network monitoring capability, and a denial of access to network control capability.

19. The method of claim 18, wherein in response to the step of classifying said network event, said method further comprises the steps of:

updating an existing conditions database with indicia of said network event;

determining a latest network topology associated with said network event; and

updating a network topology database with said latest network topology.

20. The method of claim 19 further comprising the steps of:

determining whether said BOF event also causes a BOS event;

determining whether said BOS event also causes a BOF; and

reporting at least one of said BOF event and BOS event.

21. The method of claim 20 further comprising the steps of:

categorizing said BOF event;

determining at least one corrective action procedure associated with said BOF event; and reporting at least one of a network element and a communications link associated with said BOF event, and said at least one corrective action procedure.

22. The method of claim 20, wherein in an instance where said network degradation event is associated with a breach-of security event, said method further comprises the steps of:

categorizing said breach of security event;

determining at least one corrective action procedure associated with said breach of security event; and

displaying at least one of a network element and a communications link associated with said breach-of security event, and said at least one corrective action procedure.

23. The method of claim 19 further comprising the steps of:

initiating a new network event upon resolving said network degradation event;

removing said network degradation event from said existing conditions database; and

reporting said network degradation event as a resolved event.

24. Apparatus for managing a network, comprising:

means for detecting occurrence of a network event, said network event having associated with it a network condition comprising at least one of an unplanned macro-event and a planned macro-event related to at least one of a network element and a communication link of said network;

means for classifying said network event as being at least one of a network element failure, a communications link failure, and a security breach; and

means for identifying said network event as a network degradation event in response to at least one network event exceeding a network degradation threshold.

25. The apparatus of claim 24, further comprising:

means for sending an alert to normalize said network degradation event.

26. The apparatus of claim 24, wherein said means for identifying comprises:

means for defining said network degradation event as a brink of failure (BOF) event in an instance where said event is at least one of a type determined to cause a failure of at least one network element within a predetermined time interval, to affect at least one of a critically defined network functionality, and to affect a number of end users exceeding a predetermined threshold level.

27. The apparatus of claim 26, wherein said means for identifying further comprises:

means for defining said network degradation event as a breach-of-security (BOS) event in an instance where said network event exploits a security vulnerability resulting in at least one of an unauthorized access, an unauthorized modification or compromise, a denial of access to information, a denial of access to network monitoring capability, and a denial of access to network control capability.

28. The apparatus of claim 24, wherein said means for classifying further comprises:

updating an existing conditions database with indicia of said network event;

determining a latest network topology associated with said network event; and

updating a network topology database with said latest network topology.

29. The apparatus of claim 26 further comprising:

means for determining whether said BOF event also causes a BOS event;

means for determining whether said BOS event also causes a BOF; and

means for reporting at least one of said BOF event and BOS event.

30. The apparatus of claim 29 further comprising:

means for categorizing said BOF event;

means for determining at least one corrective action procedure associated with said BOF event; and

means for reporting at least one of a network element and a communications link associated with said BOF event, and said at least one corrective action procedure.

31. The apparatus of claim 29, wherein in an instance where said network degradation event is associated with a breach-of security event, said apparatus further comprises:

means for categorizing said breach of security event;

means for determining at least one corrective action procedure associated with said breach of security event; and means for displaying at least one of a network element and a communications link associated with said breach-of security event, and said at least one corrective action procedure.

32. The apparatus of claim 29 further comprising:

means for initiating a new network event upon resolving said network degradation event;

means for removing said network degradation event from said existing conditions database; and

means for reporting said network degradation event as a resolved event.

33. The apparatus of claim 32, wherein resolving said network degradation event further comprises at least one of:

means for resolving said BOF event, such that the BOF event and a BOS condition are cleared; and

means for resolving said BOS event, such that the BOS event and a BOF condition are cleared.

34. A network management system for characterizing at least one network degradation event in a communications network, comprising:

a processing unit having access to at least one storage device;

at least a portion of said at least one storage device having a program product configured to:

detect occurrence of a network event, said network event having associated with it a network condition comprising at least one of an unplanned macro-event and a planned macro-event related to at least one of a network element and a communication link of said network;

classify said network event as being at least one of a network element failure, a communications link failure, and a security breach; and

identify said network event as a network degradation event in response to at least one network event exceeding a network degradation threshold.